UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/849,318	05/19/2004	Paul Gassoway	063170.7177	5789

5073 7590 09/12/2008

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2136	

NOTIFICATION DATE	DELIVERY MODE
09/12/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com
glenda.orrantia@bakerbotts.com

Office Action Summary	Application No.	Applicant(s)	
	10/849,318	GASSOWAY, PAUL	
	Examiner	Art Unit	
	OSCAR A. LOUIE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 June 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Pre-Appeal Brief filed on 06/18/2008, PROSECUTION IS HEREBY REOPENED. New grounds of rejection are set forth below.

Examiner Note

The examiner notes that Claim 19 recites "a computer" but the applicant's Specification does not appear to provide a clear definition as to what "a computer" comprises. However, the examiner notes that it is reasonable to expect one of ordinary skill in the art at the time of the applicant's invention to understand a computer to comprise at least a processor/microprocessor with memory (i.e. recording medium, random access memory, etc.), thus 35 U.S.C. 101 has not been invoked by the applicant with respect to Claim 19 as of the current claim language.

Claim Objections

2. Claims 1, 7, 13, & 19 are objected to because of the following informalities:

- Claim 1 line 1 recites the term "for" which should be "…of…";
- Claim 7 line 1 recites the term "for" which should be "…configured to…";
- Claim 13 lines 3, 4, 6-8, 10, & 12 recite "code for" which should be "…code written to…";
- Claim 19 line 1 recites the term "for" which should be "…configured to…";
- Claim 19 line 2 recites "being operable to" which should be "…configured to…";

Claim scope is not limited by claim language that suggests or makes optional but does not require steps to be performed, or by claim language that does not limit a claim

to a particular structure. However, examples of claim language, although not exhaustive, that may raise a question as to the limiting effect of the language in a claim are:
(A) " adapted to " or "adapted for " clauses;
(B) " wherein " clauses; and
(C) " whereby " clauses.

The determination of whether each of these clauses is a limitation in a claim depends on the specific facts of the case. In Hoffer v. Microsoft Corp., 405 F.3d 1326, 1329, 74 USPQ2d 1481, 1483 (Fed. Cir. 2005), the court held that when a "whereby' clause states a condition that is material to patentability, it cannot be ignored in order to change the substance of the invention." Id. However, the court noted (quoting Minton v. Nat 'l Ass 'n of Securities Dealers, Inc., 336 F.3d 1373, 1381, 67 USPQ2d 1614, 1620 (Fed. Cir. 2003)) that a "whereby clause in a method claim is not given weight when it simply expresses the intended result of a process step positively recited.'" Id.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 7 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

- Claim 7 recites "a system for maintaining computer security" comprising "means for" however, it appears that the "means for" do not comprise hardware and are merely computer software modules, thereby invoking 35 U.S.C. 101;

Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component. (The definition of "data structure" is "a physical or logical relationship among data elements, designed to support specific data manipulation functions." The New IEEE Standard Dictionary of Electrical and Electronics Terms 308 (5th ed. 1993).) "Nonfunctional descriptive material" includes but is not limited to music, literary works, and a compilation or mere arrangement of data.

Both types of "descriptive material" are nonstatutory when claimed as descriptive material per se, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive

*material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare In re Lowry, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994)(discussing patentable weight of data structure limitations in the context of a statutory claim to a data structure stored on a computer readable medium that increases computer efficiency) and >In re< Warmerdam, 33 F.3d *>1354,< 1360-61, 31 USPQ2d *>1754,< 1759 (claim to computer having a specific data structure stored in memory held statutory product-by-process claim) with Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure per se held nonstatutory)*

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-5, 7-11, 13-17, 19-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya (US-6279113-B1) in view of Nakae et al. (US-20040172558-A1).

Claim 1, 7, 13, & 19:

Vaidya discloses a method/a computer recording medium including computer executable code for maintaining security of a computer system and a system for maintaining computer security comprising,

- "providing access to a database of signatures" (i.e. "the data repository 12 includes a database handler 26 which polls the data collectors 10 for intrusion detection data and stores the data for future reference") [column 5 lines 47-50];
- "each signature including a signature certainty value" (i.e. "The attack signature profile type can be either simple, sequential or a timer/counter based") [column 7 lines 2-4];

- "receiving data" (i.e. "The remote network 24 is connected to the LAN 11 and is equipped with a data collector 10 which monitors work stations located on the remote
- network 24 and transmits network security data specific to the remote network back to the data repository 12. Both the remote network 24 and the LAN 11 are connected to the global communications network referred to as the Internet") [column 5 lines 39-46];
- "comparing the received data with the database of signatures" (i.e. "The attack signature profiles are adapted for detecting network data patterns associated with network intrusions which include unauthorized attempts to access network objects, unauthorized manipulation of network data, including data transport, alteration or deletion, and attempted delivery of malicious data packets capable of causing a malfunction in a network object") [column 5 lines 33-39];
- "filtering the data based on the system certainty value and the signature certainty value of a signature matching the received data" (i.e. "If in step 64 the data collector 10 determines that the data packet is not associated with a network intrusion, the data collector continues to monitor data in step 58. If a network intrusion is detected, the reaction module is notified in step 66. The reaction module 38 takes steps to trace the application session associated with the data packet, to terminate the session, and/or to notify the network administrator") [column 7 lines 4-11];

but, Vaidya does not explicitly disclose,

- "determining an initial system certainty value for the computer system," although Nakae et al. do suggest obtaining a confidence level, as recited below;

- "increasing the system certainty value if the received data does not match a signature in the database," although Nakae et al. do suggest increasing a confidence level, as recited below;
- "decreasing the system certainty value if the received data matches a signature in the database," although Nakae et al. do suggest decreasing a confidence level, as recited below;

however, Nakae et al. do disclose,

- "obtains a confidence level" [page 10 para 174 line 3];
- "the relevant confidence level is increased" [page 10 para 176 lines 3-4];
- "For example, when having received an alert denoting the source IP address "12. 34. 56. 78" through the control interface 106, the defense rule determination section 1001 interprets it as subtracting one (1) from the confidence level for the IP address "12. 34. 56. 78" and instructs the confidence management section 502/701 to decrement the corresponding confidence level by one" [page 13 pare 239 lines 1-7];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "determining an initial system certainty value for the computer system" and "increasing the system certainty value if the received data does not match a signature in the database" and "decreasing the system certainty value if the received data matches a signature in the database," in the invention as disclosed by Vaidya for the purposes of utilizing confidence levels in conjunction with various intrusion detection schemes (i.e. anomaly based, signature based, etc.) to filter incoming network traffic (i.e. incoming traffic from the Internet).

Claims 2, 8, 14, & 20:

Vaidya and Nakae et al. disclose a method/a computer recording medium including computer executable code for maintaining security of a computer system and a system for maintaining computer security, as in Claims 1, 7, 13, & 19 above, their combination further disclosing,

- "the data that does not match a signature in the database is forwarded to its destination" (i.e. "indicating which network objects are not permitted to access other network objects") [column 6 lines 34-35].

Claims 3, 9, 15, & 21:

Vaidya and Nakae et al. disclose a method/a computer recording medium including computer executable code for maintaining security of a computer system and a system for maintaining computer security, as in Claims 1, 7, 13, & 19 above, but Vaidya does not explicitly disclose,

- "the increased or decreased certainty value becomes the initial system value," although Nakae et al. do suggest updating confidence levels, as recited below;

however, Nakae et al. do disclose,

- "as shown in the following formula (4), a constant C (>1) is added to the confidence level c[n] to produce an updated confidence level c[n+1]" [page 10 para 176 lines 4-6];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the increased or decreased certainty value becomes the initial system value," in the invention as disclosed by Vaidya for the purposes of updating the confidence level of a requester to determine if the requester exceeds a threshold, thereby determining if a requester is permitted or denied access to the network.

Claims 4, 10, 16, & 22:

Vaidya and Nakae et al. disclose a method/a computer recording medium including computer executable code for maintaining security of a computer system and a system for maintaining computer security, as in Claims 1, 7, 13, & 19 above, their combination further disclosing,

- "the data comprises a packet of data" (i.e. "data packets") [column 5 line 38].

Claims 5, 11, 17, & 23:

Vaidya and Nakae et al. disclose a method/a computer recording medium including computer executable code for maintaining security of a computer system and a system for maintaining computer security, as in Claims 1, 7, 13, & 19 above, but Vaidya does not explicitly disclose,

- "the filtering further comprises forwarding the data if the signature certainty value is less than the system certainty value," although Nakae et al. do suggest the confidence level exceeding the threshold value, as recited below;
- "the filtering further comprises discarding the data if the signature certainty value is greater than the system certainty value," although Nakae et al. do suggest blocking access when the confidence does not exceed the threshold, as recited below;

however, Nakae et al. do disclose,

- "After the confidence level c has exceeded the threshold value T, the IP packets of the access from the ordinary host 302 are guided to the server 401 on the internal network 4" [page 11 para 193 lines 16-19];
- "This causes input IP packets to be continuously guided to the decoy unit. Thereafter, when detecting an attack corresponding to "intrusion" or "destruction", the permanent access blocking is made active" [page 14 para 249 lines 7-11];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the filtering further comprises forwarding the data if the signature certainty value is less than the system certainty value" and "the filtering further comprises discarding the data if the signature certainty value is greater than the system certainty value," in the invention as disclosed by Vaidya for the purposes of providing a determination as to whether a requester is permitted or denied access to the network according to a confidence level.

6. Claims 6, 12, 18, 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vaidya (US-6279113-B1) in view of Nakae et al. (US-20040172558-A1) and in further view of Moran (US-7032114-B1).

Claims 6, 12, 18, & 24:

Vaidya and Nakae et al. disclose a method/a computer recording medium including computer executable code for maintaining security of a computer system and a system for maintaining computer security, as in Claims 1, 7, 13, & 19 above, but their combination do not explicitly disclose,

- "the step of forwarding further comprises generating a message log to indicate that data matching a signature was forwarded," although Moran does suggest an event record, as recited below;

however, Moran does disclose,

- "an intrusion detection system comprises a mechanism for checking timestamps, configured to identify backward and forward time steps in a log file, filter out expected

time steps, correlate them with other events, and assign a suspicion value to a record associated with an event" [column 4 lines 28-33];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the step of forwarding further comprises generating a message log to indicate that data matching a signature was forwarded," in the invention as disclosed by Vaidya and Nakae et al. for the purposes of recording timed information for future further analysis.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to the applicant's disclosure.

a. Esbensen (US-5796942-A) – logs;

b. Brock et al. (US-20030009693-A1) - dynamic intrusion detection for computer systems;

c. Bardsley et al. (US-20030061514-A1) - limiting the output of alerts generated by an intrusion detection sensor during a denial of service attack;

d. Coleman et al. (US-20050037733-A1) - method and system for wireless intrusion detection prevention and security management;

e. Debar et al. ("Aggregation and Correlation of Intrusion-Detection Alerts") – confidence levels;

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/OAL/
09/08/2008

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136